ONLINE ILLEGAL BEHAVIOUR

AND THE MOCKERY

MIRJAM DISSEL

INTRODUCTION

Going from analog to digital has affected the way we store information, the way we shop, the way we meet friends. The we way we live our lives, including the way we indulge ourselves in illegal activities. This causes the government to make changes in the legal system and in law enforcement. This obviously has consequenses for the people involved.

I can divide the people affected into three different groups:
1. There are people who do illegal things online. This evokes counteractions by the government, there will be more and differents kind of surveillance.
2. Then there are the people who 'accidentally' get caught in this new system.
3. The people who mock the system.

In this essay I would like to explore these different categories, to see how new media changes the ways of unorganized criminals and what consequences this has for the way we are monitored/ surveilled by the government and websites, and what countermeasures users use to deceive or mock this system, and why they do this. I'm going to guide you through this by using current examples.

A QUICK TOUR ON THE CHANGE FROM ANALOG TO DIGITAL.

From 1986 to 2007, Martin Hilbert and Priscila López estimated the world's technological capacity to store, communicate, and compute information, tracking 60 analog and digital technologies. The outcome shows us how much we are indeed living in a digital age. (Hilbert and López, 2011)

"'In the year 2000, 75% of all information was still in analog format, mainly analog video cassettes (like VHS),' Hilbert says." And although analog technologies will always remain to exist, in 2002, just two years later, digital information became dominant, they estimated. "In 2007, 94% of our global technological memory consisted of digital bits and bytes." (Andrea Leontiou, 2011) This is a big shift in the way we store data and how we can access this information.

As said: all this information overload gives us new possibilities. Also in the criminal scene. Seemingly anonymous we can spy on our neighbours whereabouts, cyberbully a random person whose information was found on the web, or order prohibited substances.

HOW UNORGANIZED CRIME HAS SHIFTED

Patrick Hess (2002, p.24) defines cyber crimes as following: "harmful acts committed from or against a computer or network - differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal."

The last point is the most interesting one. The crime are often not easily identifiable as illegal, this happens for several reasons: They work around the law, in such a new terrain as the internet, laws are outdated and cannot apply in certain cases. With no physical presence it is hard to define the jurisdiction, again, laws on this keep getting out of date. Since online, it is much easier to be discovered than offline, you must hide your illegal practices from surveillance in a new and resourceful ways, for example by disguising as legal practices. One can do this by using an already existing platform, using it the way it was intented, just with disguised goods.

In 2009, a worried mom in Phoenix, USA, discovered her son was acting strangely and irritated. She snooped online and monitored him for a while, discovering different candies for sale on his Myspace profile: purple Pokeballs and white Machintosh Thizzles. She googled and found out these candies actually have ecstasy in them, and warned the police. (Marquez, 2009; Pillreports.com, 2010)

Sharing drugs amongst friends on social networking websites such as Myspace or Facebook is one thing, finding regular dealing through forums or chatboxes is another. Mail Order Marijuana (MOM) is another concept towards buying drugs online. It allows you to pay a certain person (preferably in cash via the regular, analog mail), and then receive marijuana in a letter or package back. This can go back and forth for a long time, and these dealers have a big clientele. Personally, I've been redirected to a website that sells joint holders, so you don't have to hold them with your fingers. Basically, these items are clips with knotted scoubidou craftworks at the end. My sister could make them in 10 seconds. The website however, is selling them for $60 and they offer stealth shipping, after you've physically mailed the ordering form. You get the idea. (Fingerclips, 2011)
"[These] websites are hidden from search engines like Google. Most experts agree that the given the scale and anonymity of the internet, the online drug trade is unstoppable. 'It's not policeable. There are not enough cops in the world to monitor all the communications and digital commerce that's going on.'" (Guardian, 2004)

Every once in a while a distributor of marijuana does get caught, for sending marijuana to an undercover cop, or sometimes the mail gets intercepted at the post distribution centre. But the recipients then try to find new dealers again on their forums.
Caution is key when involving oneself in such practices, on these same forums, many stories warn you about scams (and so, even the criminal circuit gets exploited by other criminals) and before you know it you'll find yourself with an empty wallet and no marijuana in the mail. Because of course, we do not hold any rights, nor can we apply the ten commandments of online shopping: such as checking the domainregister, paypal support, face to face transactions, etc. The same policies that restrict our privacy is not there to protect us.

When moving our offline businesses to online, we often subscribe to websites and agree to policies. When we try to resell a concert ticket because we cannot attend the concert after all, there are a bunch of new rules we have to abide. When in the olden days, we asked all of our friends if they wanted to buy a ticket, now we subscribe to ebay and try to reach a bigger audience. In the Netherlands it is legal to resell a ticket, but in Italy for example, it is not. (Ebay, 2011) You have to disguise your ticket as a previous event, autographed by the singer (in order to justify the high price for a piece of paper), so you can try to resell it. Since everybody in Italy knows this, it is no problem for the users. The policy is not working though, but should it?
When you are forced to refrain from something you would normally do without thinking, you are going to find ways around it, because the policy seems ridiculous and unfair. Even though in real life the same rules apply, the police or website cannot look into your home, which enables you to do these things unpunished.

A lot of times we are also on the other side: the side of the victim. On a daily basis people are getting threatened, stalked, scammed.
Although some of us are really stupid, others are just very unfortunate, most of the time not realizing what they get themselves into when giving out personal information or trusting random people online, providing others with the opportunity to penetrate into their private lives and benefit from it.
In March of this year the legal case Bonhomme vs. St. James served. (Internetcases, 2011a) Paula Bonhomme believed to be in a commited (online) relationship with Jesse James (who was actually portrayed by her forum friend Janna St. James), and after spending $10,000 worth of gifts, the man supposedly died. She later found out, Janna St. James, deceived her and created multiple online personas (posing as "Jesse's" family) to make the 'Jesse story' plausible.

This is a very one on one encounter, but what about all our data that is freely accessible? Many people who are subscribed to online service Foursquare (you can 'check in' at real life places, earning points and unlocking badges, thus exploring the city in a new way) also check in at their own home. This provides a great risk. Anyone in the area can access this data, and if you automatically let the application post it to your (often public) Facebook wall, it is easy to see if you're going to be away from home long. If you're far away from home or if you've just checked into a restaurant, you will not see the comfort of your designer chair again for at least 2 hours, or perhaps forever.
"It may seem a small number, but 2% of people have been burgled when out and about after posting details of their whereabouts on social media. If growth of location-based services continues, the likelihood is that this figure will rise." (Home Insurance, 2010)

HOW IS SURVEILLANCE CHANGING IN REGARD TO THE SHIFT IN CRIME FROM OFFLINE TO ONLINE?

"[In 2020,] computers will be much faster than they are today, with equal or greater advances in data storage capacity, data transfer rates (both wired and wireless), and miniaturization. These factors will foster many new technology applications that will be seamlessly integrated into every facet of life. Given the rapid rate of change we can expect over the next 15 years and the new capabilities and opportunities that it will bring to policing, business as usual is not an option. More powerful computers do not simply allow us to do what we've always done faster; more powerful computers allow us to do things we never thought possible." (Schafer, p.79)

Foucault's panopticon surveillance prohibits the user to act natural, because he knows he's being watched, while the superpanopticon construction (there is no tower in the middle, no guards to be seen, Poster, 1990) relies on invisible surveillance. All the prisoners/users are being watched, they just do not see it.

Right now the legal system is closely monitoring whatever is happening online, they search on their own initiative (and gather IP adresses) by looking on google for criminal activities, and they often catch youth who videotaped things like underage drinking, vandalizing, assault, and then upload it somewhere like Youtube. Other times the law enforcements start an online investigation when presented with a case in court, or when tipped off by someone. And sometimes they are even satisfied with another person's inventions to deceive the system.

In the case of zwartrijdenov, a twitter account that anyone can update with the current public transit ticket controls around Utrecht, the transport companies aren't bothered at all that the commuters know there is a control, "at least they will pay" so they say. (RTVUtrecht, 2011)

When the authorities do hit a serious case, like the one about "Jesse James", it leads to changes in the law. The "Megan Meier Cyberbullying Prevention Act" by U.S. Representative Linda T. Sánchez was created after the suicide of thirteen-year old Megan Meier, who believed she was in a relationship with a boy, who was actually her friend's mom, disguised on Myspace.
The bill criminalizes the use of electronic communications if "the intent is to coerce, intimidate, harass, or cause substantial emotional distress to a person."The bill has drawn some criticism, it would infringe the constitutional right of freedom of speech. (Cato.org, 2011) It's a bit of push and a bit of pull.
This happens also on other terrains dealing with digital data. With the case of Sony vs. George Hotz in March 2011, with Hotz being accused of breaching the Digital Millennium Copyright Act by providing people with iPhone hacks and the Playstation 3 jailbreak, Sony was given access to the PS3 hacker's PayPal records, as well as the the IP's from his own website, his Twitter account, Youtube, and Google. With that, all of the IP's of the users are also exposed, who knows to what cause? (Arstechnica, 2011)

So, how does it actually work, finding out one's IP adress, aren't these identifiable numbers protected? It's actually very easy for law enforcement to find out who you are, just by looking at your IP adress. Even if in the first place it is not possible directly from the provider, after a few tricks they can still find out.
In January 2011, a porn company in the U.S. sued 59 anonymous defendants it knew only by IP address, for violation of the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA) and copyright infringement.
But since it did not know it's defendants, it had to first find that out.
1. A subpoena to the defendants' internet service providers would reveal the needed information. But these ISPs, being governed by the Cable Communications Policy Act of 1984, could not turn over their subscribers' information without a court order.
2. Only until after the initial conference with the defendant the previous subpoena can start. But of course this is not possible since the plaintiff did not know its defenders.
3. The court has to step in and decide about the court order. Different courts have different standards in providing this court order. (Internetcases, 2011b)

PEOPLE WHO UNSUSPECTEDLY GET CAUGHT IN THE SYSTEM.

The internet is no playground, the watchdogs are keeping a close eye on us and all of a sudden, you can become a victim of this policing.

In contrast to the real world, prohibited activities you do online are suddenly out in the open, for all the public to see, making it easier for the Department of Justice to find all minor offences and turn them into something that may have a great effect on your life.
"Barnes (2004) states that computer networks often promote a false sense of privacy among users, often because correspondents do not actually see the others who are reading their profiles or messages therefore users have a false sense of security about the content of the information they provide to others via photos or text in online settings." (Watson, Smith and Driver, 2006)
This can have radical results:

A couple of students found out what the concequences of surveillance through Facebook were: "a university in Atlanta, USA, charged certain Facebook group members with 'conduct violations' after the members posted information regarding their alcohol use on-campus (Buckman, 2005) and four students at Northern Kentucky University (Buckman, 2005) were charged after posting photos of themselves consuming alcohol in a dorm room." (Watson, Smith and Driver, 2006)
One could argue that it is just plain stupidity what these students did, and that it is just as much common knowledge that facebook is being monitored as that there are CCTV camera's and other security on campus. Still there is a difference: the physical presence of these surveillance instruments has an immediate and deep impact, that alters the way we handle situations. On Facebook there is not a two-way webcam stream with the board of directors staring into your dorm. You can't see who visited your profile. Even if you have all the privacy setting on 'alert alert danger danger', chances are your friends are going to upload pictures of you of that party you went to last week.

Even in court your Facebook pictures could set you back. In February 2011 a case served whether Theresa Purvis had been wrongfully denied Social Security benefits. Purvis was claiming her disability was based on her asthma, but when the judge did some researching of her own, she discovered one profile picture on "what is believed to be" Purvis' Facebook page where she "appears to be" smoking. (Internetcases, 2011c)
How forgiving should the internet be? How reliable are those pictures anyway? The asthma patient was "apparently" smoking, is that good enough? How does the judge know how old these pictures are? Can you decide on the basis of a picture

wether it's even a real cigarette or an electronic one? What is the worth of such a picture?

I realise we should not be so oblivious to the information we put online, but the way it comes back around is just cruel.
Another student got expelled over something seemingly trivial as a Facebook picture. The nursing student was posing with a placenta, after she asked the professor if she could take the picture. She was later reinstated, after she sued the college. The court said that pictures are taken to be viewed, and the professor, in allowing the picture to be taken, thus consented the picture to be posted online. (Internetcases, 2011d)

When possibilities are becoming endless, there are a lot of things we might didn't think of. Of course, it is foolish of the professor to think that the student was only going to do some nice scrapbooking with the placenta picture, or just keep it in the dark domains of her hard disk. But other times it is not so obvious. When you visit a website that contains information on how to do certain illegal activities (downloading mp3's, flashing the firmware of your phone), or even a normal newspaper website, your anonymity could be at risk.
The Dutch Ministry of Security and Justice inquired all the IP adresses of the newspaper website "de Culemborgse Courant" between January 1 and 4, 2010. The paper was devoting a lot of space to a certain case, and the Ministry was interested in witness reports of people who were leaving comments on the website. The publisher did not reply, up till two requests, before the Ministry gave it a rest. (Nu, 2010)
In February 2010 parliamentary questions were asked by MP Marianne Thieme (PvdD) to the Minister of Justice (Ernst Hirsch Ballin). She asks in which cases the Ministry may collect generic data, if and how civilians are in danger, if the mere fact that someone in a period of time visited a particular website, can justify the IP data from that person to be claimed. If not, is the Ministry willing to protect the privacy of Internet users better than now is the case? These are all very valid questions, and important if something like this occurs again. Unfortunately, she did not receive an answer. (Ikregeer, 2010)

And so incidents like this happen over and over: back in 2006 there was a mom from the north of the Netherlands who tried to get rid of her baby on Marktplaats. Of course it was a joke, but Marktplaats filed a report with the police, and eventually they found the "mom": a fifteen-year old boy who put a picture of his baby sister online for fun. Also the seventeen-year old girl who out of frustration recently tweeted she was going to bomb her school got suspended from school, after being arrested by the police. (Nu, 2011a) Days later a thirteen-year old boy does the same thing and he gets taken in for interogation and the attorney general still has to decide if he needs to go to the children's judge. (Nu, 2011b)

It's great that we are preventing another high school drama, and letting go of your frustration in your own personal diary is very different from blurting it all out in your public twitter account, and young people should be aware of this. I would probably get arrested immediately for all the terrible things I've wished upon the people around me when I was in elementary school, luckily, it's all in a paper diary and not online, but if twitter existed back then, and I hadn't know, who knows, maybe I would have done the same thing.

So how far should we let the government control our businesses? And if we let them, can they really help us? Are they reliable, are they good at what they do? And how can they monitor every forum discussion and protect us from people who try to take our identities, people like "Jesse James", how are they going to police cyberbullying (which often result in real life problems, such as depression or suicide).

MOCKING THE SYSTEM

In as a reaction to all this surveillance, some kids are trying to joke around with their invisible audiences. At George Washington University, USA, "college students played a prank on the watchful campus police. They advertised a massive beer blast on Facebook, but when campus police arrived to bust them, all they found was [40 students and a table with] cake and cookies decorated with the word 'beer' (Hass 2006)."(Boyd, 2007)

Also, many celebrities have been pronounced dead over the years by twitter hoaxes, Zach Braff (Scrubs), Eddie Murphy, Mick Jagger (Aerosmith) and recently Dutch singer Jody Bernal have been reported dead. Dutch newspaper journalist Wilma Nanninga of the Telegraaf also believed it to be real and tweeted that a Swiss press agency said Bernal had died after a snowboarding accident. (Volkskrant, 2011)

And if you happen to be in the possession of a picture you made of a police officer you can upload it to Wim Holsappel's website. (politiefoto.nl) This is a counteraction to the police taking pictures of South-Holland youth without their permission and gathering data about them. These small paybacks do not really result in any type of influence on the legal system.

So why do these people mock the system? There's enough fun stuff for them to do, in real life and online, why is it so exciting to abuse the surveillance that is supposed to keep them all safe?

It's not all about having fun and pulling a prank, it's a counteraction towards an evergrowing grip of all sorts of organisations monitoring our every move. There is no grey zone anymore, the space where we can do the little things that make us happy, but from a legal perspective aren't allowed. The grey zone is needed by the society to function, to have a breathing space to feel comfortable. This was available in the analog world, when police couldn't be everywhere at the same time, monitoring every space, every corner. When they are indeed monitoring everything, you have to watch your steps, everytime you take a step. This causes anxiousness, people get caught in the system. Therefore people mock the system, they fear with more and more control there is no more freedom, we'll get trapped. There are too many 'false positives' popping up. We need the freedom to fix someone's computer, receive 50 euros for it and not pay taxes over it. We need to park our car and not pay for a ticket and quickly buy some cigarettes race off again. If it wasn't like this we would be very limited, if every small crime would be seen and punished, then every minute we would have to think about our actions and the consequences.

The online surveillance system is still very much in an early state. It's mostly a direct translation from the professional law enforcement model, used in the analog world, "It is set to protect against a public police force which reacts to committed crime by collecting evidence for prosecution" (Kozlovski, p.14), while we need a shift in policing as a reaction to the new crime scene: cyber-policing, which will be more effective and will rule out the errors that cause innocent people to get caught in the system.

Untill that day, people are going to mock the system, by screwing it up, legally, providing false data and misinformation, to play with the authorities, untill they make a change.

CONCLUSION

How do I feel about all of this? To me, is it really a crime to sell concert tickets? These little everyday crimes we commit suddenly become traceable, because, as you know, the internet does not forget. It's open and it's searchable. Disguising these 'crimes' to hide the fact that you are doing something illegal makes it sound even worse. [rephrase] But is it? Is the system not just forcing us to find these new innovative ways of doing the activities we would normally do as well? Hasn't everyone had a beer long before they were allowed to? Is the system not asking for us to mock it's infantile ways of controlling us?

Now that surveillance on the streets is at an ultimately high level (in Rotterdam alone there are 370 camera's, 100 to be added. And another astonishing 2000 by RET, the local transport company, who sometimes work together with the police, when asked (VPRO, 2010)), and we are also heavily being watched in our digital businesses, is there any room left for privacy? A well known argument is 'if you have nothing to hide, what are you afraid of?'. If I did nothing wrong, why are they looking at me? The data being collected about loitering youth, the police is criminalizing people who have done nothing wrong yet. Do they have any boundaries? With all the data that has been gathered so far, I am afraid that new technologies (which, may I add, are developing RAPIDLY), will be able to combine all this data, have intelligent ways of adding more information to this stack of data and hey, maybe we can go back to 1897 when Cesare Lombroso published his L'Uomo Delinquente (The Criminal Man), with new insights on how facial features determine whether you are a 'born criminal' or not. These criminals would have a 'strange appearance'. Did I mention there are camera's who can detect 'odd behaviour' and that we are also living in a time where these scans are fully automatic? The police is looking online, even when you are inside your home you can still get into trouble for something trivial as surfing a particular website.

It shouldn't be that I don't want to sign online petitions against an anti-gay iphone app because I'm afraid my data is going to pop up somewhere someday, and that the person who is looking at it is not going to like it and will refuse me of a service, or of a job.

And it shouldn't be that i'm afraid to buy a multiple finger ring online, because I'm afraid somewhere someday, someone is going to find out and think I bought brass knuckles, which happen to be illegal in the Netherlands, which turns me in to an offender.

Since we cannot look into the future, and cannot know who are going to be our leaders and what they will decide to do with our information, I think we should be cautious in allowing all of our lives being documented. Even if you have nothing to hide, even if you did nothing wrong, in retrospect you could still be screwed when they change the laws and are able to put all the pieces together. Insurance companies are already looking at your habits on social media and location-based services when handling your burglary claim. And when you get lungcancer in 20 years, the insurance company might decide not to cover you because their algorithm shows you have been smoking in over 20% of your social network pictures in the decade before. Is that fair?

REFERENCES

Hilbert, M. and López, P., 2011. The World's Technological Capacity to Store, Communicate, and Compute Information. Science Express [online] 10 February 2011. Available at: <http://www.sciencemag.org/content/early/2011/02/09/science.1200970.abstract> [Accessed 4 March 2011]

Leontiou, A., 2011. Humanity's Shift from Analog to Digital Nearly Complete. Tech News Daily [online] 10 February 2011. Available at: <http://www.technewsdaily.com/humanitys-shift-from-analog-to-digital-nearly-complete-2145/> [Accessed 4 March 2011]

Hess, P., 2002. Cyberterrorism and Information War. New Delhi: Anmol Publications.

Pillreports.com [online] Available at: <http://www.pillreports.com> [Accessed March 4 2011]

Guardian [online] 31 January 2004. Available at: <http://www.guardian.co.uk/politics/2004/jan/31/1>

Fingerclips [online] Available at: <http://www.fingerclips.com/> [Accessed March 25 2011]

Ebay [online] Available at: <http://pages.ebay.it/help/policies/event-tickets.html> [Accessed at March 25 2011]

Internetcases, 2011a [online] Available at: <http://blog.internetcases.com/about/library/bonhomme-v-st-james-n-e-2d-2011-wl-901966-ill-app-2-dist-march-10-2011/>

Legal & general insurance limited, 2010. Home Insurance Digital Criminal Report, 2010

Schafer, J.A.. Policing 2020: Exploring the Future of Crime, Communities, and Policing

Poster, M., 1990. The Mode of Information

RTVUtrecht, 23 February 2011. [online] Twitter voor zwartrijders opgezet. Available at: <http://www.rtvutrecht.nl/nieuws/334412>

Cato.org, September 30 2009 [online] Available at: <http://www.cato.org/pub_display.php?pub_id=12221>

arctechnica [online] Available at: <http://arstechnica.com/gaming/news/2011/03/judge-gives-sony-access-to-ps3-hackers-paypal-records.ars>

Internetcases, 2011b [online] Federal court applies Seescandy.com test to unmask anonymous defendants in copyright and privacy case . Available at: <http://blog.internetcases.com/2011/02/03/subpoena-attorney-anonymous-isp-unmask-john-doe-copyright-infringement/>

Watson, S. W.; Smith, Z.; Driver, J , 2006. Alcohol, Sex and Illegal Activities: An Analysis of Selected Facebook Central Photos in Fifty States'

Internetcases, 2011c [online] Judge uses Facebook to research litigant. Available at: <http://blog.internetcases.com/2011/03/09/judges-use-facebook-to-research-litigants/>

Internetcases, 2011d [online] College must reinstate nursing student who posted placenta picture on Facebook. Available at: <http://blog.internetcases.com/2011/01/22/chicago-facebook-attorney-lawyer-college-must-reinstate-nursing-students-who-posted-placenta-pics-on-facebook/>

Nu.nl, February 15 2010. http://www.nu.nl/internet/2184870/culemborgse-courant-staat-internetadressen-niet-af.html

Ikregeer.nl, February 19 2010. http://ikregeer.nl/document/kv-2010Z03240?format=pdf

Nu.nl 2011a, February 17 2011. http://www.nu.nl/binnenland/2448932/meisje-opgepakt-dreiging-bomaanslag-school.html

Nu.nl 2011b, March 10 2011. http://www.nu.nl/binnenland/2464890/jongen-13-aangehouden-dreigtweets.html

Boyd, D., May 2007. http://kt.flexiblelearning.net.au/tkt2007/edition-13/social-network-sites-public-private-or-what/

van Lier, H., Volkskrant.nl March 6 2011. http://www.volkskrant.nl/vk/nl/2690/Opmerkelijk/article/detail/1856150/2011/03/06/Wilma-Nanninga-verspreidt-nepbericht-Jody-Bernal-overleden.dhtml

http://www.wimholsappel.nl/politiefoto/website/about.php

Kozlovski, N. A Paradigm Shift in Online Policing – Designing Accountable Policing

VPRO, Holland Doc, 2010. Wat nou privacy? http://www.hollanddoc.nl/kijk-luister/maatschappij/privacy.html?playurn=urn:vpro:media:program:5260402&currentPage=2